Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

On the Product of Two Substitutions.

By G. A. Miller.

The main object of this paper is to prove the following

Theorem.—*If l, m, n are any three integers greater than unity, of which we call the greatest k, it is always possible to find three substitutions (L, M, N) of $k+2$ or some smaller number of elements and of orders l, m, n respectively such that $LM = N$.*

The following lemmas may be employed to prove this theorem:

Lemma I. *If two circular substitutions (S_1, S_2) have an odd number of consecutive elements in common, while all their other elements are distinct, these common elements may be so arranged that the product $S_1 S_2$ is a circular substitution which involves all the elements of S_1 and S_2 except an arbitrary even number of the common elements.*

Let

$$S_1 = (a_1 \ldots . a_{2\alpha+1} \ldots . a_{2n+1} \ldots . a_k)^* \text{ and}$$
$$S_2 = (a_{2\alpha+1} \ldots . a_1 a_{2\alpha+2} \ldots . a_{2n+1} a_{k+1} \ldots . a_l).\dagger$$

The product $S_1 S_2$ will contain: 1st, all the common elements that have odd subscripts larger than 2α; 2nd, all the elements of S_1 that are not contained in S_2; 3rd, all the common elements that have even subscripts larger than 2α; 4th, all the elements of S_2 that are not contained in S_1. Hence

$$S_1 S_2 = (a_{2\alpha+1} a_{2\alpha+3} \ldots . a_{2n+1} a_{2n+2} \ldots . a_k a_{2\alpha+2} a_{2\alpha+4} \ldots . a_{2n} a_{k+1} \ldots . a_l).$$

It is clear that the number (2α) of the common elements that do not appear in this product may be made to vary from 0 to $2n$.

---

* Throughout this article it is supposed that the omitted elements have for subscripts all the consecutive numbers in order, between the given limits, unless the contrary is indicated by the elements which are written out.

† When $\alpha = n$, the elements $a_{2\alpha+2} \ldots . a_{2n+1}$ do not occur.

Lemma II. *If two circular substitutions (S_1, S_2) have an even number of consecutive elements in common while all their other elements are distinct, these common elements may be so arranged that the product $S_1 S_2$ is a circular substitution which involves all the elements of S_1 and S_2 except any arbitrary odd number of the common elements.*

Let

$$S_1 = (a_1 \ldots\ldots a_{2\alpha} \ldots\ldots a_{2n} \ldots\ldots a_k) \text{ and } S_2 = (a_{2\alpha} \ldots\ldots a_1 a_{2\alpha+1} \ldots\ldots a_{2n} a_{k+1} \ldots\ldots a_l).$$

The product $S_1 S_2$ will contain: 1st, all the common elements that have even subscripts larger than $2\alpha - 1$; 2nd, all the elements of S_1 that are not contained in S_2; 3rd, all the common elements that have odd subscripts larger than 2α; 4th, all the elements of S_2 that are not contained in S_1. Hence

$$S_1 S_2 = (a_{2\alpha} a_{2\alpha+2} \ldots\ldots a_{2n} a_{2n+1} \ldots\ldots a_k a_{2\alpha+1} a_{2\alpha+3} \ldots\ldots a_{2n-1} a_{k+1} \ldots\ldots a_l).$$

When $2\alpha = 2n = k = l$, the number of elements in the product $S_1 S_2$ should be one according to the lemma. Such a substitution is clearly impossible, the corresponding product being identity. From these two lemmas we observe that the elements of two circular substitutions (S_1, S_2) may be so chosen that their product is a circular substitution whose order is any arbitrary number that may be obtained by diminishing the sum of the orders of S_1 and S_2 by any odd positive number which is less than twice the smaller one of these two orders.

Lemma III. *If a circular substitution (S_1) has an odd number (greater than unity) of elements in common with a substitution (S_2) which is composed of a transposition and a circular substitution, the common elements may be so arranged that the product $S_1 S_2$ is a circular substitution which contains all the elements of S_1 and S_2 except any arbitrary odd number (less than the total number) of the common elements.*

Let

$$S_1 = (a_1 \ldots\ldots a_{2\alpha+2} \ldots\ldots a_{2n+1} \ldots\ldots a_k) \text{ and}$$

$$S_2 = (a_{2\alpha+2} a_{2\alpha+3})(a_{2\alpha+1} \ldots\ldots a_1 a_{2\alpha+4} \ldots\ldots a_{2n+1} a_{k+1} \ldots\ldots a_l).^*$$

The product $S_1 S_2$ will contain: 1st, all the common elements that have odd subscripts larger than 2α; 2nd, all the elements of S_1 that are not contained in

---

[*] The elements $a_{2\alpha+4} \ldots\ldots a_{2n+1}$ are omitted when $2\alpha + 3$ has its maximal value, viz., $2n + 1$.

S_2; 3rd, all the common elements that have even subscripts larger than $2\alpha + 2$; 4th, all the elements of S_2 that are not contained in S_1. Hence

$$S_1 S_2 = (a_{2\alpha+1} a_{2\alpha+3} \ldots . a_{2n+1} a_{2n+2} \ldots . a_k a_{2\alpha+4} a_{2\alpha+6} \ldots . a_{2n} a_{k+1} \ldots . a_l).$$

The common elements which do not occur in $S_1 S_2$ are clearly $a_1 \ldots . a_{2\alpha}$ and $a_{2\alpha+2}$. When there is only one such element, it is a_2, α being equal to zero.

Lemma IV. *If a circular substitution* (S_1) *has an even number* (*greater than zero*) *of elements in common with a substitution* (S_2) *which is composed of a transposition and a circular substitution, the common elements may be so arranged that the product* $S_1 S_2$ *is a circular substitution which contains all the elements of* S_1 *and* S_2 *except an arbitrary even number* (*less than the total number*) *of the common elements.*

We shall first suppose that the number of common elements ($2n$) exceeds two, and that the elements which do not occur in $S_1 S_2$ are $a_1 \ldots . a_{2\alpha-1}$ and $a_{2\alpha+1}$ ($\alpha \neq 0$). It is clear that $\alpha + 1 \ngtr n$.

Let

$$S_1 = (a_1 \ldots . a_{2\alpha} \ldots . a_{2n} \ldots . a_k) \text{ and}$$
$$S_2 = (a_{2\alpha+1} a_{2\alpha+2})(a_{2\alpha} \ldots . a_1 a_{2\alpha+3} \ldots . a_{2n} a_{k+1} \ldots . a_l).^*$$

The product $S_1 S_2$ will contain: 1st, all the common elements that have even subscripts greater than $2\alpha - 1$; 2nd, all the elements of S_1 that are not contained in S_2; 3rd, all the common elements that have odd subscripts greater than $2\alpha + 1$; 4th, all the elements of S_2 that are not contained in S_1. Hence

$$S_1 S_2 = (a_{2\alpha} a_{2\alpha+2} \ldots . a_{2n} a_{2n+1} \ldots . a_k a_{2\alpha+3} a_{2\alpha+5} \ldots . a_{2n-1} a_{k+1} \ldots . a_l).$$

If all the common elements are to appear in $S_1 S_2$, we may use the following substitutions:

$$S_1 = (a_1 \ldots . a_{2n} \ldots . a_k) \text{ and } S_2 = (a_1 a_3)(a_2 a_4 a_5 \ldots . a_{2n} a_{k+1} \ldots . a_l).$$

Finally, if S_1 and S_2 have only two common elements, they may have the following forms:

$$S_1 = (a_2 a_1 a_3 a_4 \ldots . a_k) \text{ and } S_2 = (a_2 a_{k+1})(a_1 a_{k+2} \ldots . a_l).$$

From the last two lemmas we observe that the elements of two substitutions (one (S_1) being circular and the other, (S_2), consisting of a transposition and a circular substitution) may be so chosen that the product $S_1 S_2$ is a circular substitution whose order is any arbitrary number that may be obtained by diminishing

---

[*] The elements $a_{2\alpha+3} \ldots . a_{2n}$ do not occur when $\alpha + 1 = n$.

the sum of the degrees of S_1 and S_2 by any even positive integer (excluding 0) which is less than twice the smaller of these two degrees. If the degree of S_2 is supposed to be even, we may deduce the following result from these lemmas: The elements of S_1 and S_2 may be so chosen that their product is a circular substitution whose order is any arbitrary integer that may be obtained by diminishing the sum of the orders of S_1 and S_2 by any even positive integer (including 0) which does not exceed twice the smaller of these orders. Combining this result with the one stated after Lemma II, we have the following: If one of two arbitrary integers is even, it is always possible to find two substitutions whose orders are these integers respectively and the sum of whose degrees does not exceed the sum of their orders by more than two, such that their product is a circular substitution whose order is any arbitrary number that may be obtained by diminishing the sum of the two given integers by any integer (0 included) which does not exceed twice the smaller of the given integers.

We are now prepared to prove the given theorem without much difficulty. Since the relation $LM = N$ is equivalent to $MN^{-1} = L^{-1}$, as well as to $N^{-1}L = M^{-1}$, we may assume $l \leqq m \leqq n$. This will be done in what follows. Hence we have

$$n = \alpha m + \beta = \alpha m + k(l-1) + \varepsilon, \quad m = \gamma l + \delta, \quad \delta < l, \quad \varepsilon < l - 1, \quad \beta < m.$$

We shall first consider the case when l is even, and represent M as follows:

$$M = (a_1 \ldots . a_m)(a_{m+1} \ldots . a_{2m}) \ldots . (\,) \ldots . (a_{(\alpha-1)m+1} \ldots . a_{\alpha m}).$$

When $\alpha > 1$, we let

$$L = (a_1 a_{\alpha m+1})(a_2 a_{\alpha m+2}) \ldots . (\,) \ldots . (a_\beta a_{\alpha m+\beta})(a_m a_{m+1})(a_{2m} a_{2m+1}) \ldots . (\,) \ldots . \\ (a_{(\alpha-1)m} a_{(\alpha-1)m+1} \ldots . a_{(\alpha-1)m+l-1}).$$

When $\alpha = 1$ and $\beta > l$ we let

$$L = (a_1 a_{m+1})(a_2 a_{m+2}) \ldots . (\,) \ldots . (a_{\beta-l+1} a_{m+\beta-l+1})(a_m a_{m+\beta-l+2} \ldots . a_{m+\beta}).$$

When $\alpha = 1$ and $\beta \leqq l$, the proper substitutions were determined above. In what follows we may, therefore, confine our attention to the cases when l is an odd number. We shall assume, unless the contrary is stated, that M has always the given value and confine our attention to the determination of suitable values for L.

When α is even and $\varepsilon = 1$, we may employ the given M, and the following L_1 for L:

$$\begin{aligned} L_1 = (a_1\, a_{\alpha m+1} \ldots\ldots a_{\alpha m+l-1})(a_2\, a_{\alpha m+l} \ldots\ldots a_{\alpha m+2(l-1)}) \ldots\ldots (\ ) \ldots\ldots \\ (a_k\, a_{\alpha m+(k-1)(l-1)+1} \ldots\ldots a_{\alpha m+k(l-1)})(a_m\, a_{\alpha m+\beta}\, a_{m+1}\, a_{m+2} \ldots\ldots a_{m+l-2}) \\ (a_{2m}\, a_{2m+1}\, a_{3m+1} \ldots\ldots a_{3m+l-2}) \ldots\ldots (\ ) \ldots\ldots \\ (a_{(\alpha-2)m}\, a_{(\alpha-2)m+1}\, a_{(\alpha-1)m+1} \ldots\ldots a_{(\alpha-1)m+l-2}). \end{aligned}$$

When α is even and ε is odd and greater than 1, we multiply L_1 by the cycle $(a_{k+1} \ldots\ldots a_{k+l-\epsilon+1}\, a_{\alpha m+k(l-1)+1} \ldots\ldots a_{\alpha m+\beta-1})$ and use the product for L. When α and ε are even, we replace the element $a_{\alpha m+\beta}$ in L_1 by the element $a_{\alpha m+\beta+1}$ and multiply the result by the cycle

$$(a_{k+2}\, a_{\alpha m+\beta+2}\, a_{k+1}\, a_{k+3} \ldots\ldots a_{k+l-\epsilon-1}\, a_{\alpha m+k(l-1)+1} \ldots\ldots a_{\alpha m+\alpha}.)^*$$

This product is to be used for L. It remains to consider the cases when both α and l are odd. When $\varepsilon = 0$ (α and l being odd), we employ the following L_2 for L in the equation $LM = N$:

$$\begin{aligned} L_2 = (a_1\, a_{\alpha m+1} \ldots\ldots a_{\alpha m+l-1})(a_2\, a_{\alpha m+l} \ldots\ldots a_{\alpha m+2(l-1)}) \ldots\ldots (\ ) \ldots\ldots \\ (a_k\, a_{\alpha m+(k-1)(l-1)+1} \ldots\ldots a_{\alpha m+k(l-1)})(a_m\, a_{m+1}\, a_{2m+1} \ldots\ldots a_{2m+l-2}) \\ (a_{3m}\, a_{3m+1}\, a_{4m+1} \ldots\ldots a_{4m+l-2}) \ldots\ldots (\ ) \ldots\ldots \\ (a_{(\alpha-2)m}\, a_{(\alpha-2)m+1}\, a_{(\alpha-1)m+1} \ldots\ldots a_{(\alpha-1)m+l-2}). \end{aligned}$$

If ε is even and greater than 0,.we may obtain a suitable value for L by multiplying L_2 by the cycle $(a_{k+1} \ldots\ldots a_{k+l-\epsilon}\, a_{\alpha m+k(l-1)+1} \ldots\ldots a_{\alpha m+\beta})$. When each of the three numbers α, l, ε is odd while m is even, we may use the following M_3, L_3 for M and L respectively:

$$M_3 = (a_1 \ldots\ldots a_m)(a_{m+1} \ldots\ldots a_{2m}) \ldots\ldots (\ ) \ldots\ldots (a_{(\alpha-1)m+1} \ldots\ldots a_{\alpha m})(a_{\alpha m+1}\, a_{\alpha m+2}),$$
$L_3 = L_2$ multiplied by $(a_{k+1} \ldots\ldots a_{k+l-\epsilon+1}\, a_{\alpha m+2} \ldots\ldots a_{\alpha m+\beta})$.

When each of the four numbers α, l, ε, m is odd and $\varepsilon < l - 2$, we may employ the following M_4, L_4 for M and L respectively:

$M_4 = M$,
$L_4 = L_2$ multiplied by the cycle $(a_{k+2}\, a_{\alpha m+\beta+2}\, a_{k+1}\, a_{k+3} \ldots\ldots a_{k+l-\epsilon-2}\, a_{\alpha m+k(l-1)+1} \ldots\ldots a_{\alpha m+\beta+1})$.†

When each of the four numbers α, l, ε, m is odd, $l - 2 = \varepsilon$ and $m > l$, we may employ the following M_5, L_5 for M and L respectively:

---

* When $l = 3$, this cycle consists of its first three elements, when $\varepsilon = 0$ the elements $a_{\alpha m+k(l-1)+1} \ldots a_{\alpha m+\beta}$ are to be omitted.

† When $l = \varepsilon + 4$, the elements $a_{k+1} \ldots\ldots a_{k+l-\epsilon-2}$ are to be omitted.

$M_5 = M$,
$L_5 = L_2$ multiplied by the two cycles $(a_{k+1}\, a_{\alpha m+k(l-1)+1} \,\ldots\, a_{\alpha m+\beta+1})$
$(a_{k+3}\, a_{\alpha m+\beta+2}\, a_{k+2}\, a_{k+4} \,\ldots\, a_{k+l})$.*

Finally, when the four numbers α, l, ε, m are odd and $l - 2 = \varepsilon = m - 2$, we may employ the following M_6, L_6 for M and L respectively:

$$M_6 = (a_1 \ldots a_m)(a_{m+1} \ldots a_{2m}) \ldots (\;) \ldots (a_{\alpha m+1} \ldots a_{(\alpha+1)m}),$$
$$L_6 = (a_m\, a_{m+1}\, a_{2m+1} \ldots a_{3m-2})(a_{3m}\, a_{3m+1}\, a_{4m+1} \ldots a_{5m-2}) \ldots (\;) \ldots$$
$$(a_{(\alpha-2)m}\, a_{(\alpha-2)m+1}\, a_{(\alpha-1)m+1} \ldots a_{\alpha m-2})(a_{\alpha m}\, a_{\alpha m+3}\, a_{\alpha m+1}\, a_{\alpha m+4} \ldots a_{(\alpha+1)m}).\dagger$$

We have now found suitable substitutions in each of the possible cases, and we never employed more than $n + 2$ different elements. Hence, the proof of the given theorem is complete. There is clearly no substitution except identity whose order is less than two. This was the reason for assuming that each of the numbers l, m, n is greater than unity. With respect to abstract-group theory the given theorem may be stated as follows: It is possible to find three operators whose orders are any three arbitrary numbers greater than unity such that the product of two of them is the third operator. Hence, we can choose in a triply infinite number of ways the orders of three operators which satisfy the condition that one of them is the product of the other two. While an operator of a finite order always generates a cyclical group of a finite order it follows directly from the given theorem that two operators of any given finite orders greater than unity, which are otherwise unrestricted, generate a group of an infinite order that contains operators of every possible finite order.

CORNELL UNIVERSITY.

---

* When $l = 3$, this cycle consists of its first three elements.

† When $m = 3$, this cycle contains only its first three elements.